Theoretical Computer Science 102 (1992) 307–328
Elsevier

The multiplicative complexity of quadratic boolean forms

R. Mirwald and C.P. Schnorr

Fachbereich Mathematik/Informatik, Universität Frankfurt, Robert Mayerstrasse 68, D-6000 Frankfurt, Germany

Communicated by M.S. Paterson
Received June 1987
Revised October 1990

Abstract

Mirwald, R. and C. P. Schnorr, The multiplicative complexity of quadratic boolean forms, Theoretical Computer Science 102 (1992) 307–328.

Let the multiplicative complexity $L(f)$ of a boolean function f be the minimal number of $\wedge$-gates that are sufficient to evaluate f by circuits over the basis $\wedge, \oplus, 1$. We characterize the multiplicative complexity $L(f)$ of quadratic boolean forms f; it is half the rank of an associated matrix. Two quadratic boolean forms $f; g$ have the same complexity $L(f)=L(g)$ iff they are isomorphic by a linear isomorphism. We characterize computational independence of two quadratic boolean forms f_1, f_2 in the sense that $L(f_1, f_2)=L(f_1)+L(f_2)$.

1. Summary

Determining the circuit complexity of boolean functions is a major challenge to complexity theory. In this paper we consider the multiplicative complexity $L(f)$ of boolean functions f; $L(f)$ is the minimal number of $\wedge$-gates (binary multiplications) that are sufficient to evaluate f by a circuit over the basis $\wedge, \oplus, 1$. The constant 1 and $\oplus$, the addition modulo 2, are free of charge. For the first time we evaluate the complexity of entire classes of boolean functions, that of quadratic forms. An n-ary quadratic (boolean) form is a polynomial $f=\bigoplus_{i\neq j} a_{ij}x_ix_j$ with coefficients $a_{ij}\in\mathbb{Z}_2=\mathrm{GF}(2)$ and boolean variables $x_1,\ldots,x_n$. It is helpful to analyze first the level-one multiplicative complexity $L_1(f)$ of quadratic forms; $L_1(f)$ is the minimal number of $\wedge$-gates that are sufficient to evaluate f by a circuit that has only one level of $\wedge$-gates.

In Section 2 we summarize basic concepts from complexity theory and from linear algebra.

In Section 3 we determine the multiplicative complexity of single quadratic forms. We characterize in Theorem 3.4 the L_1-complexity in various ways. Theorem 3.5 shows that every circuit which computes the quadratic form f with $L(f)$ many $\wedge$-gates has at most one level of $\wedge$-gates. As a consequence, $L(f)=L_1(f)$ holds for all quadratic forms f; furthermore, $L(f)$ can easily be determined since it equals half the rank of an associated matrix. We conclude that $L(f)=t$ iff f is isomorphic to the *canonical form* $\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$. With an n-ary boolean form f we associate the *dual domain* $D(f)$. $D(f)$ is the smallest linear subspace U of n-ary linear boolean forms such that f, up to a linear form, can be written as a polynomial with inputs in U. For all quadratic forms f we have $L(f)=\frac{1}{2}\dim D(f)$. For two quadratic forms f_1, f_2 we have $L(f_1 \oplus f_2)=L(f_1)+L(f_2)$ iff $D(f_1 \oplus f_2)$ is the direct sum of $D(f_1)$ and $D(f_2)$ (Corollary 3.8). The fraction of $2n$-ary quadratic forms f that have maximal multiplicative complexity $L(f)=n$ is greater than one third and at most one half of all $2n$-ary quadratic forms (Theorem 3.10).

In Section 4 we characterize the multiplicative complexity of pairs of quadratic forms. We first analyze the L_1-complexity and we subsequently prove that the complexity measures L and L_1 coincide for pairs of quadratic forms. We prove that for any two quadratic forms f_1, f_2 there exists a quadratic form g such that

$$L_1(f_1, f_2)=L(f_1 \oplus g)+L(f_2 \oplus g)+L(g)$$

$$L(f_i)=L(f_i \oplus g)+L(g) \quad \text{for } i=1,2.$$

These equations describe an L_1-minimal circuit for f_1, f_2 consisting of two L-minimal circuits for f_1 and f_2 with a common subcircuit for g. Theorem 4.1 establishes the existence of g. Theorem 4.2 characterizes for a canonical form $f=\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$ the set of quadratic forms g with $L(g)=1$ that *help* in computing f in the sense that $L(f \oplus g)=L(f)-1$. Theorem 4.4 characterizes pairs of quadratic forms f_1, f_2 that are *computationally independent* in the sense that $L_1(f_1, f_2)=L(f_1)+L(f_2)$. For given quadratic forms f_1 and f_2 that are not computationally independent we can find in polynomial time a quadratic form g with $L(g)=1$ which helps in computing both f_1 and f_2 (Theorem 4.4). We prove in Theorem 4.5 that the maximal L_1-complexity of pairs of n-ary quadratic forms is $\lfloor 3n/4 \rfloor$. Finally, Theorem 4.6 shows that the complexity measures L_1 and L coincide for pairs of quadratic forms.

In Section 5 we consider the multiplicative complexity of sets $\{f_1, \ldots, f_r\}$ of quadratic boolean forms. We show that the complexity of almost all sets of r n-ary quadratic boolean forms has a lower bound $L(f_1, \ldots, f_r) \geq n\sqrt{r}/3$ (Theorem 5.1). Therefore, determining the multiplicative complexity of sets of quadratic boolean forms could lead to nonlinear circuit complexity lower bounds, a decisive breakthrough in complexity theory. It is open whether such lower bounds are provable or whether they are unprovable for fundamental reasons as has been conjectured in [9]. Sets of quadratic boolean forms seem to be the right test point for either proving

nonlinear circuit complexity lower bounds or understanding the reasons they may be unprovable. We show in Theorem 5.2 that the level-one multiplicative complexity of sets of r n-ary quadratic boolean forms is bounded from above and from below by the rank of corresponding $n \times n \times r$-tensors. Therefore, proving a lower bound to the L-complexity of sets of quadratic boolean forms requires proving a lower bound to the rank of the corresponding tensor. So far there is no example of a sequence of $n \times n \times r$ tensors with coefficients in $\mathbb{Z}_2$ such that a lower rank bound has been proven which is nonlinear in $n+r$. Proving such a nonlinear lower rank bound seems to be a difficult task. By Theorem 5.2 this task is still easier than proving nonlinear circuit complexity lower bounds for sets of quadratic boolean forms.

2. Preliminaries

Let $B_n = \{f: \mathbb{Z}_2^n \to \mathbb{Z}_2\}$ be the ring of n-ary boolean functions with the binary operations $\oplus$ (addition modulo 2), $\wedge$ (multiplication, logical and). According to the canonical isomorphism, we identify the ring B_n with the factor ring $\mathbb{Z}_2[x_1, \ldots, x_n]/(x_1 - x_1^2, \ldots, x_n - x_n^2)$. Here $\mathbb{Z}_2[x_1, \ldots, x_n]$ is the ring of formal polynomials in the formal variables $x_1, \ldots, x_n$ with coefficients in the Galois field $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$, and $(x_1 - x_1^2, \ldots, x_n - x_n^2) \subset \mathbb{Z}_2[x_1, \ldots, x_n]$ is the ideal generated by the polynomials $x_1 - x_1^2, \ldots, x_n - x_n^2$. The equivalence class $x_i + (x_1 - x_1^2, \ldots, x_n - x_n^2) \subset B_n$ of the formal variable x_i is the corresponding *boolean variable* in B_n which is again denoted by x_i. We associate with the boolean functions $f_1, \ldots, f_r$ the linear subspace $\langle f_1, \ldots, f_r \rangle \subset B_n$ generated by $f_1, \ldots, f_r$, and which is called the *span* of $f_1, \ldots, f_r$. Let $B_{n,d} \subset B_n$ be the subspace $\langle x_{i_1} \cdot \ldots \cdot x_{i_d} \mid 1 \leqslant i_1 < \cdots < i_d \leqslant n \rangle$ of n-ary *boolean forms* of degree d; $B_{n,2}$ ($B_{n,1}$) is the linear space of quadratic (linear) forms. The *degree* of a boolean function $f = \bigoplus_{d=0}^{n} f_d$ with $f_d \in B_{n,d}$ is the maximal number d such that $f_d \neq 0$; notation $\deg f$. All quadratic forms in this paper will be boolean quadratic forms. We write $f = g \pmod{B_{n,1}}$ if $f \oplus g \in B_{n,1}$. To abbreviate formulae we suppress all $\wedge$-symbols. We use the letters f, g, h, k for boolean functions, u, v, w for linear forms, x, y for boolean variables, a, b, c for boolean constants, z for boolean vectors, U, V for subspaces of $B_{n,1}$, and E, F for subspaces of $\mathbb{Z}_2^n$.

The *multiplicative complexity* $L(f_1, \ldots, f_r)$ of a set of boolean functions $f_1, \ldots, f_r \in B_n$ is the minimal integer t for which there exist boolean functions g_i, h_i, k_i in B_n for $i = 1, \ldots, t$ such that

(2.1) $h_1, k_1 \in \langle x_1, \ldots, x_n \rangle$, $g_1 = h_1 k_1$ and

$h_i, k_i \in \langle g_1, \ldots, g_{i-1}, x_1, \ldots, x_n \rangle$, $g_i = h_i k_i$ for $i = 2, \ldots, t$.

(2.2) $f_1, \ldots, f_r \in \langle g_1, \ldots, g_t, x_1, \ldots, x_n, 1 \rangle$.

This recursion describes a *circuit* for $f_1, \ldots, f_r$ with input variables $x_1, \ldots, x_n$. It is sufficient that the constant 1 can be added in the final step (2.2).

For quadratic forms $f_1, \ldots, f_r \in B_{n,2}$ the *level-one multiplicative complexity* $L_1(f_1, \ldots, f_r)$ is the minimal integer t for which there exist linear forms $u_i, v_i \in B_{n,1}$ for $i = 1, \ldots, t$ such that

$$(2.3) \quad f_1, \ldots, f_r \in \langle u_1 v_1, \ldots, u_t v_t, x_1, \ldots, x_n \rangle.$$

Obviously, $L(f_1, \ldots, f_r) \leqslant L_1(f_1, \ldots, f_r)$ for all $f_1, \ldots, f_r \in B_{n,2}$.

If $T: \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ is a linear mapping and $f \in B_m$ is a boolean function, we let $fT \in B_n$ denote the function defined by $(fT)(z) = f(Tz)$. If $f \in B_{m,2}$ is a quadratic form then fT may not be a form but there is a unique quadratic form $g \in B_{n,2}$ which differs from fT by some linear form, i.e. $fT = g \pmod{B_{n,1}}$. We say T *transforms* f into g, even though fT and g differ by a linear form. We always have $L(fT) \leqslant L(f)$ since a circuit for f can be transformed into a circuit for fT by replacing each variable x_i by the linear form $x_i T$. We call two quadratic forms $f, g \in B_{n,2}$ *isomorphic*, if there is a linear isomorphism $T: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ such that $fT = g \pmod{B_{n,1}}$. Clearly, if f and g are isomorphic then $L(f) = L(g)$.

Let $M_{m,n}(\mathbb{Z}_2)$ denote the set of $m \times n$ matrices over $\mathbb{Z}_2$. We identify points $z \in \mathbb{Z}_2^n$ with column vectors in $M_{n,1}(\mathbb{Z}_2)$ and linear forms $u \in B_{n,1}$ with row vectors in $M_{1,n}(\mathbb{Z}_2)$. Then the value $u(z)$ coincides with the matrix product uz. We associate with a matrix $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in M_{n,n}(\mathbb{Z}_2)$ the quadratic form $f_A = \bigoplus_{i \neq j} a_{i,j} x_i x_j \in B_{n,2}$. Then the corresponding boolean function $f_A: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies

$$f_A(z) = z^{\mathrm{T}} A z \quad \text{for all } z \in \mathbb{Z}_2^n,$$

provided that the diagonal entries of A are all zero. The matrix A *represents* the quadratic form f_A.

The mapping $A \mapsto f_A$ yields a vector space homomorphism $\psi: M_{n,n}(\mathbb{Z}_2) \to B_{n,2}$, $\psi(A) = f_A$. The kernel of ψ is the subspace of symmetric matrices including the diagonal matrices. ψ is surjective. We have

$$f_A = f_B \Leftrightarrow A \oplus B \text{ is symmetric} \Leftrightarrow A \oplus A^{\mathrm{T}} = B \oplus B^{\mathrm{T}}$$

for all $A, B \in M_{n,n}(\mathbb{Z}_2)$. Here A^{T} is the transpose of the matrix A. We see that the matrices $A \oplus A^{\mathrm{T}}$ are in 1–1 correspondence with the quadratic forms. We call $A \oplus A^{\mathrm{T}}$ the matrix *corresponding* to f_A.

We represent a linear mapping $T: \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ by the matrix $\tau \in M_{m,n}(\mathbb{Z}_2)$ which satisfies

$$T(z) = \tau z \quad \text{for all } z \in \mathbb{Z}_2^m.$$

Let $f_A \in B_{m,2}$ be a quadratic form and let $T: \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ be a linear mapping. Then there is a uniquely defined quadratic form $f_B \in B_{n,2}$ such that $f_B = f_A T \pmod{B_{n,1}}$. We show that $f_B = f_{\tau^{\mathrm{T}} A \tau}$. For this let the diagonal entries of A be all zero. Then we have

$$f_A(z) = z^{\mathrm{T}} A z \qquad \text{for all } z \in \mathbb{Z}_2^m,$$

$$f_A(Tz) = z^{\mathrm{T}} \tau^{\mathrm{T}} A \tau z \qquad \text{for all } z \in \mathbb{Z}_2^n.$$

This shows that the matrix $\tau^{\mathrm{T}}(A \oplus A^{\mathrm{T}})\tau$ corresponds to the quadratic form $f_A T \pmod{B_{n,1}}$.

The *dual mapping* $T^*: B_{m,1} \to B_{n,1}$ of a linear mapping $T: \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ is defined by

$$T^*(u) = uT \quad \text{for all } u \in B_{m,1}.$$

The dual mapping T^* and the mapping T are represented by the same matrix $\tau \in M_{m,n}(\mathbb{Z}_2)$. We have for all row vectors $u \in B_{m,1}$ and all column vectors $z \in \mathbb{Z}_2^n$

$$T(z) = \tau z, \qquad T^*(u) = u\tau.$$

3. Complexity classes and isomorphism classes of quadratic forms

We first analyze the L_1-complexity of single quadratic forms and we later on prove that the complexity measures L and L_1 coincide for single quadratic forms.

Lemma 3.1. *Suppose the quadratic form f can be written $f = \bigoplus_{i=1}^{t} u_i v_i \pmod{B_{n,1}}$ with $u_i, v_i \in B_{n,1}$. If $L_1(f) = t$ then $u_1, \ldots, u_t, v_1, \ldots, v_t$ are linearly independent and f is isomorphic to $\bigoplus_{i=1}^{t} x_{2i-1} x_{2i}$.*

Proof. Suppose $L_1(\bigoplus_{i=1}^{t} u_i v_i) = t$ holds for the linearly dependent linear forms $u_1, \ldots, u_t, v_1, \ldots, v_t$. Without loss of generality (w.l.o.g.), let $u_t = \bigoplus_{i<t} a_i u_i \oplus \bigoplus_{i=1}^{t} b_i v_i$ with $a_i, b_i \in \mathbb{Z}_2$. We have

$$\bigoplus_{i=1}^{t} u_i v_i = \bigoplus_{i=1}^{t-1} (u_i \oplus b_i v_t)(v_i \oplus a_i v_t) \pmod{v_t}$$

and thus $L_1(\bigoplus_{i=1}^{t} u_i v_i) < t$. This contradicts the assumption.

If $u_1, v_1, \ldots, u_t, v_t$ are linearly independent there is a linear isomorphism T on $\mathbb{Z}_2^n$ defined by $T^*(u_1) = x_1$, $T^*(v_1) = x_2$, ..., $T^*(u_t) = x_{2t-1}$, $T^*(v_t) = x_{2t}$. T transforms $\bigoplus_{i=1}^{t} u_i v_i$ into $\bigoplus_{i=1}^{t} x_{2i-1} x_{2i}$. □

Lemma 3.2. *For every boolean $n \times n$ matrix $A = (a_{i,j})$ with $\bigoplus_{i=1}^{t} x_{2i-1} x_{2i} = f_A = \bigoplus_{i,j} a_{i,j} x_i x_j$ we have $\frac{1}{2}\mathrm{R}(A \oplus A^{\mathrm{T}}) = t$, where $\mathrm{R}(A \oplus A^{\mathrm{T}})$ denotes the rank of $A \oplus A^{\mathrm{T}}$.*

Proof. We have $\frac{1}{2}\mathrm{R}(A \oplus A^{\mathrm{T}}) = t$ for the matrix $A = (a_{i,j})$ with $a_{2i-1,2i} = 1$ *for* $i = 1, \ldots, t$ and $a_{i,j} = 0$ for all other entries. The claim follows from the equivalence $f_A = f_B$ iff $A \oplus A^{\mathrm{T}} = B \oplus B^{\mathrm{T}}$. □

Lemma 3.3. *For every boolean $n \times n$ matrix B we have $\frac{1}{2}\mathrm{R}(B \oplus B^{\mathrm{T}}) = L_1(f_B)$.*

Proof. Let $L_1(f_B) = t$. Then there exist linear forms $u_1, \ldots, u_t, v_1, \ldots, v_t$ such that $f_B = \bigoplus_{i=1}^{t} u_i v_i \pmod{B_{n,1}}$. By Lemma 3.1 the forms $u_1, \ldots, u_t, v_1, \ldots, v_t$ are linearly

independent and f_B is isomorphic to $\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$. Let A be a boolean $n \times n$ matrix such that $f_A = \bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$. Since f_A, f_B are isomorphic, there exists a regular matrix τ such that $f_B = f_{\tau^T A \tau} \pmod{B_{n,1}}$, and thus we have $B \oplus B^T = \tau^T(A \oplus A^T)\tau$. By Lemma 3.2 we have

$$t = \tfrac{1}{2}R(A \oplus A^T) = \tfrac{1}{2}R(B \oplus B^T). \qquad \square$$

We immediately obtain from the above Lemmata the following Theorem.

Theorem 3.4. *Let* $f \in B_{n,2}$ *and* $u_1, \ldots, u_t, v_1, \ldots, v_t \in B_{n,1}$ *such that* $f = \bigoplus_{i=1}^{t} u_i v_i \pmod{B_{n,1}}$. *Then the following conditions are equivalent:*

(1) $L_1(f) = t$.

(2) $u_1, \ldots, u_t, v_1, \ldots, v_t$ *are linearly independent,*

(3) f *is isomorphic to the canonical form* $\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$,

(4) *for every boolean* $n \times n$ *matrix* A *with* $f_A = f$ *we have* $\frac{1}{2}R(A \oplus A^T) = t$.

The equality $L(f_A) = \frac{1}{2}R(A \oplus A^T)$ is based on the boolean congruence $x^2 = x$; it does not hold for quadratic forms in $\mathbb{Z}_2[x_1, \ldots, x_n]$. By Theorem 3.4(d) the rank of $A \oplus A^T$ is even for all boolean $n \times n$ matrices A. The matrices $A \oplus A^T$ range over all symmetric boolean matrices that have zero diagonal elements. These matrices $(b_{i,j}) = A \oplus A^T$ are skew symmetric, i.e. $b_{i,j} = -b_{j,i}$. It is well known that skew symmetric matrices have even rank..

Theorem 3.5. *Every circuit that computes some quadratic form* f *with* $L(f)$ *many* $\wedge$*-gates has at most one level of* $\wedge$*-gates.*

Proof (*by contradiction*). Let t be the minimal integer for which there is a circuit with t $\wedge$-gates that has at least two levels of $\wedge$-gates for some quadratic form f with $L(f) = t$. Consider a first $\wedge$-gate of this circuit and let this $\wedge$-gate compute the product uv of linear forms u, v. These forms must be linearly independent since otherwise we could eliminate this $\wedge$-gate. By applying a suitable isomorphism $T: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ to the entries of the circuit we can transform u, v into the variables x_1, x_2. Thus, we can assume that $u = x_1$, $v = x_2$. The restriction $x_1 = 0$ eliminates the above $\wedge$-gate from the circuit. Hence, $L(f_{|x_1=0}) \leqslant t-1$. On the other hand, we have $L(f_{|x_1=0}) \geqslant t-1$ since one $\wedge$-gate is sufficient to compute f from $f_{|x_1=0}$. This is because $f = f_{|x_1=0} \oplus x_1 w$ for some linear form w. So far we have shown that $L(f_{|x_1=0}) = t-1$.

By the minimality of t every circuit which computes $f_{|x_1=0}$ with $t-1$ $\wedge$-gates has at most one level of $\wedge$-gates. Thus, the restriction $x_1 = 0$ yields a circuit for $f_{|x_1=0}$ with only one level of $\wedge$-gates. We see that the given circuit for f, as a circuit with inputs x_1x_2 and $x_1, \ldots, x_n$, has only one level of $\wedge$-gates. Therefore, f can be written as

$$(3.1) \quad f = \bigoplus_{i=1}^{t-1} (a_i x_1 x_2 \oplus u_i)(b_i x_1 x_2 \oplus v_i) \oplus c x_1 x_2 \pmod{B_{n,1}}$$

with linear forms u_i, v_i and constants a_i, b_i, c in $\mathbb{Z}_2$. Since $\deg(f)=2$, we have

$$\deg\left(\bigoplus_{i=1}^{t-1}(a_i v_i \oplus b_i u_i)x_1 x_2\right)\leqslant 2,$$

and thus $\bigoplus_{i=1}^{t-1}(a_i v_i \oplus b_i u_i)\in\langle x_1, x_2\rangle$.

This shows that the linear forms $x_1, x_2, u_1, \ldots, u_{t-1}, v_1, \ldots, v_{t-1}$ are linearly dependent. On the other hand, we see from (3.1) that

$$f\in\langle x_1 x_2, u_1 v_1, \ldots, u_{t-1} v_{t-1}, x_1, \ldots, x_n\rangle.$$

Since the linear forms $x_1, x_2, u_1, \ldots, v_{t-1}$ are linearly dependent, Lemma 3.1 implies $L_1(f)<t$ and thus $L(f)<t$, a contradiction. □

By combining Theorems 3.4 and 3.5 we can in Theorem 3.4 replace the L_1-complexity by the L-complexity.

Theorem 3.6. *The equality $L_1(f)=L(f)$ holds for all quadratic forms f, and thus the characterization of $L_1(f)$ in Theorem* 3.4 *also applies to $L(f)$.*

In particular, by Theorem 3.4(4) the multiplicative complexity $L(f)$ of f can be found in polynomial time from the coefficients a_{ij} of the quadratic form $f=\bigoplus_{i,j}a_{ij}x_i x_j$ since $L(f)=\frac{1}{2}\mathrm{R}(A\oplus A^{\mathrm{T}})$ holds for the coefficient matrix $A=(a_{ij})_{1\leqslant i,j\leqslant n}$. From the equation $L(f)=\frac{1}{2}\mathrm{R}(A\oplus A^{\mathrm{T}})$ we can easily determine the maximal multiplicative complexity of n-ary quadratic forms:

$$\max\{L(f)\mid f\in B_{n,2}\}=\lfloor n/2\rfloor.$$

We now introduce the important notion of the dual domain of a quadratic form. Let $f\in B_{n,2}$ be a quadratic form and let $f=f_A$ for a matrix $A\in M_{n,n}(\mathbb{Z}_2)$. The *dual domain* $D(f)$ of f is the subspace of $B_{n,1}$ that is generated by the row vectors of the matrix $A\oplus A^{\mathrm{T}}$. (Here we use the identification of linear forms in $B_{n,1}$ with row vectors in $M_{1,n}(\mathbb{Z}_2)$.) This is well defined since the matrix $A\oplus A^{\mathrm{T}}$ is uniquely determined by f. In particular, the canonical form $f=\bigoplus_{i=1}^{t}x_{2i}x_{2i-1}$ has the dual domain $D(f)=\langle x_1, \ldots, x_{2t}\rangle=B_{2t,1}$. It can easily be seen that

$$\dim D(f)=2L(f)$$

holds for all quadratic forms f. For if $f=f_A$ then by definition of $D(f)$ we have $\dim D(f)=\mathrm{R}(A\oplus A^{\mathrm{T}})$. Moreover, we see from Theorem 3.4(4) and Theorem 3.6 that $\mathrm{R}(A\oplus A^{\mathrm{T}})=2L(f)$.

The following Lemma shows that $D(f)$ is the smallest subspace $U\subset B_{n,1}$ such that f can be written as $f=\bigoplus_i u_i v_i \pmod{B_{n,1}}$ with $u_i, v_i\in U$.

Lemma 3.7. *Let $f=\bigoplus_{i=1}^{t}u_i v_i \pmod{B_{n,1}}$ with linear forms $u_i, v_i\in B_{n,1}$ for $i=1,\ldots,t$. Then we have $D(f)\subset\langle u_1, v_1, \ldots, u_t, v_t\rangle$ and $D(f)=\langle u_1, v_1, \ldots, u_t, v_t\rangle$ if $t=L(f)$.*

Proof. Identifying the linear forms u_i and v_i with the corresponding row vectors we see that the quadratic form $u_i v_i \pmod{B_{n,1}}$ is represented by the matrix $u_i^{\mathrm{T}} v_i$, i.e.

$$f_{u_i^{\mathrm{T}} v_i} = u_i v_i \pmod{B_{n,1}}$$

for $i = 1, \ldots, t$. Therefore, the matrices A and $\bigoplus_{i=1}^{t} u_i^{\mathrm{T}} v_i$ represent the same quadratic form and thus

$$A \oplus A^{\mathrm{T}} = \bigoplus_{i=1}^{t} (u_i^{\mathrm{T}} v_i \oplus v_i^{\mathrm{T}} u_i).$$

This shows that every row vector of $A \oplus A^{\mathrm{T}}$ is a linear combination of $u_1, v_1, \ldots, u_t, v_t$. Hence $D(f) \subset \langle u_1, v_1, \ldots, u_t, v_t \rangle$. If $t = L(f)$ then the latter inclusion must be an equality since $\dim D(f) = 2L(f) = 2t$. □

The notion of dual domain extends in a natural way from quadratic forms to arbitrary boolean functions $f \in B_n$. For $f \in B_n$ let $D(f)$ be the smallest linear space $U \subset B_{n,1}$ such that f can be written, modulo a linear function, as a polynomial with inputs in U. It has been proved in [10] that $D(f)$ is well defined. In the case of quadratic forms this definition coincides with the above definition. An easy induction on the number of $\wedge$-gates in boolean circuits shows that the lower bound

$$L(f) \geq \tfrac{1}{2} \dim D(f)$$

holds for all boolean functions $f \in B_n$.

Corollary 3.8. *Let f_1, f_2 be quadratic forms. Then we have $L(f_1 \oplus f_2) = L(f_1) + L(f_2)$ iff $D(f_1 \oplus f_2) = D(f_1) \times D(f_2)$ where $\times$ denotes the direct sum of linear spaces.*

Proof. ("⇒"): It follows from $L(f_1 \oplus f_2) = L(f_1) + L(f_2)$ and $\dim D(f) = 2L(f)$ that

$$\dim D(f_1 \oplus f_2) = \dim D(f_1) + \dim D(f_2).$$

Therefore, and since $D(f_1 \oplus f_2) \subset \operatorname{span}(D(f_1), D(f_2))$, we must have $D(f_1 \oplus f_2) = D(f_1) \times D(f_2)$.

("⇐"): $D(f_1 \oplus f_2) = D(f_1) \times D(f_2)$ implies $L(f_1 \oplus f_2) = (\dim D(f_1 \oplus f_2))/2 = (\dim D(f_1) + \dim D(f_2))/2 = L(f_1) + L(f_2)$. □

We call two quadratic forms f_1, f_2 *strictly computationally independent* if $L(f_1 \oplus f_2) = L(f_1) + L(f_2)$. If the quadratic forms f_1, f_2 depend on disjoint sets of variables then Corollary 3.8 implies $L(f_1 \oplus f_2) = L(f_1) + L(f_2)$ and thus $L(f_1, f_2) = L(f_1) + L(f_2)$.

According to Theorems 3.4 and 3.6 every quadratic boolean form f with $L(f) = t$ is isomorphic to the canonical form $\bigoplus_{i=1}^{t} x_{2i-1} x_{2i}$. We will now describe a polynomial-time algorithm that finds a corresponding transformation.

Theorem 3.9. *Every quadratic form* $f=\bigoplus_{1\leqslant j<i\leqslant n} a_{ij}x_ix_j$ *in* B_n *can be transformed within* $2n^3$ *bit operations into the isomorphic canonical form* $\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$ *with* $t=L(f)$.

Proof. We stepwise transform f into a canonical form. Throughout these transformations f will be represented by a lower triangular matrix, i.e. $f=\bigoplus_{i,j} a_{ij}x_ix_j$ with $a_{ij}=0$ for $i\leqslant j$. We disregard linear terms arising from linear transformations. The given form satisfies for $k=m=0$ the equation

$$\bigoplus_{j\leqslant 2k}\ \bigoplus_{1\leqslant j<i\leqslant n} a_{ij}x_ix_j=\bigoplus_{i=1}^{m} x_{2i-1}x_{2i}. \tag{3.2}$$

The sequence of transformations terminates when the transformed form satisfies equation (3.2) for $k=\lfloor n/2\rfloor$ and some $m\leqslant k$.

We describe the recursion step from k to $k+1$: If $a_{ij}=0$ for all i,j with $2k<j<i$, we are finished. Otherwise, if $a_{ij}=1$, we exchange the variables x_i, x_j for x_{2k+2}, x_{2k+1} and achieve $a_{2k+2,\,2k+1}=1$. We transform f by the substitution

$$x_{2k+2}:=x_{2k+2}\oplus\bigoplus_{j>2k+2} a_{j,\,2k+1}x_j.$$

This achieves

$$a_{i,\,2k+1}:=\begin{cases}1 & \text{for } i=2k+2\\ 0 & \text{for } i>2k+2,\end{cases}$$

and transforms a_{ij} for $i>j>2k+1$ as follows:

$$a_{ij}:=a_{ij}\oplus a_{i,\,2k+1}a_{j,\,2k+2}\oplus a_{i,\,2k+2}a_{j,\,2k+1}. \tag{3.3}$$

We next substitute

$$x_{2k+1}:=x_{2k+1}\oplus\bigoplus_{j>2k+2} a_{j,\,2k+2}x_j,$$

and obtain $a_{i,\,2k+2}=0$ for all i. This terminates the recursion step within $2n^2$ bit operations. □

Theorem 3.10. *The fraction of* $2n$*-ary quadratic boolean forms* f *that satisfy* $L(f)=n$ *is* $\prod_{i=0}^{n-1}(1-2^{-2i-1})$. *This fraction is at least* 1/2 *and is smaller than* 1/3.

Proof. We have $L(f)=n$ for the quadratic form $f=\bigoplus_{1\leqslant j<i\leqslant 2n} a_{ij}x_ix_j$ iff the reduction process in the proof of Theorem 3.9 transforms f into the canonical form $\bigoplus_{i=1}^{n} x_{2i-1}x_{2i}$. This is the case iff for $k=0,\ldots,n-1$ there exists $j>2k+1$ such that $a_{j,\,2k+1}=1$ when starting the "reduction step" $k\to k+1$. The "if-part" of the claim is clear. On the other hand, if $a_{j,\,2k+1}=0$ holds for all $j>2k+1$ then the form does not depend on the variable x_{2k+1} and thus cannot be isomorphic to $\bigoplus_{i=1}^{n} x_{2i-1}x_{2i}$.

Consider the reduction process of Theorem 3.9 and let the initial coefficients a_{ij} $1 \leqslant j < i \leqslant 2n$ be independent and uniformly distributed over $\mathbb{Z}_2$. We see from the equation (3.3), that upon entry of the recursion step $k \to k+1$ the coefficients a_{ij} with $2k < j < i \leqslant 2n$ are independent. Therefore, the probability that $a_{j,2k+1} = 1$ holds for some $j > 2k+1$ is $1 - 2^{-(2n-2k-1)}$. It follows that the fraction of $2n$-ary forms that are isomorphic to $\bigoplus_{i=1}^{n} x_{2i-1} x_{2i}$ is

$$\prod_{k=0}^{n-1} (1 - 2^{-(2n-2k-1)}) = \frac{1}{2} \cdot \frac{7}{8} \cdot \frac{31}{32} \cdots \frac{2^{2n-1}-1}{2^{2n-1}}. \qquad \square$$

4. The multiplicative complexity and computational independence of pairs of quadratic forms

Due to the special field $\mathbb{Z}_2$ the complexity theory of pairs of boolean quadratic forms is rather different from the theory of pairs of bilinear forms as developed in [2, 3] for sufficiently large fields of coefficients. The multiplicative complexity of a pair of boolean quadratic forms (f_{A_1}, f_{A_2}) is closely related to the rank of its associated pair of matrices $(A_1 \oplus A_1^{\mathrm{T}}, A_2 \oplus A_2^{\mathrm{T}})$. The rank of a pair of boolean matrices has been characterized by Mirwald and Schnorr [5].

We first analyze the L_1-complexity and we later on prove that the complexity measures L and L_1 coincide for pairs of quadratic forms. For every pair of quadratic forms (f_1, f_2) we establish in Theorem 4.1 the existence of a quadratic form g such that $L_1(f_1, f_2) = L(f_1 \oplus g) + L(f_2 \oplus g) + L(g)$ and $L(f_i) = L(f_i \oplus g) + L(g)$ for $i = 1, 2$. These equations describe an L_1-minimal circuit for (f_1, f_2) consisting of two L-minimal circuits for f_1 and f_2 with a common subcircuit for g.

Theorem 4.1. *For every pair of quadratic forms $f_1, f_2 \in B_{n,2}$ there exists $g \in B_{n,2}$ such that $L_1(f_1, f_2) = L(f_1 \oplus g) + L(f_2 \oplus g) + L(g)$ and $L(f_i) = L(f_i \oplus g) + L(g)$ for $i = 1, 2$.*

Proof. Let $s = L_1(f_1, f_2)$. There exist linear forms $u_i, v_i \in B_{n,1}$ for $i = 1, \ldots, s$ such that

$$f_1, f_2 \in \langle u_1 v_1, \ldots, u_s v_s, x_1, \ldots, x_n \rangle.$$

We can permute the products $u_1 v_1, \ldots, u_s v_s$ such that

$$(4.1) \quad f_1 = \bigoplus_{i=1}^{s_1} u_i v_i \pmod{B_{n,1}}$$

$$(4.2) \quad f_2 = \bigoplus_{i=s_2+1}^{s} u_i v_i \pmod{B_{n,1}}$$

holds for some integers s_1, s_2 with $s_2 \leqslant s_1$.

If $L(f_1)=s_1$ and $L(f_2)=s-s_2$, we can take for g the function

$$g=\bigoplus_{i=s_2+1}^{s_1} u_iv_i.$$

This function g has the desired properties since $L(f_1\oplus g)=s_1$, $L(f_2\oplus g)=s-s_1$ and $L(g)=s_1-s_2$. Now suppose that either $L(f_1)<s_1$ or $L(f_2)<s-s_2$. By symmetry we can assume that $L(f_1)<s_1$. We conclude from (4.1) and Lemma 3.1 that $u_1,\dots,u_{s_1},v_1,\dots,v_{s_1}$ are linearly dependent. Thus we can assume w.l.o.g. that

$$u_{s_1}=\bigoplus_{i=1}^{s_1-1}(a_iu_i\oplus b_iv_i)\oplus b_{s_1}v_{s_1} \quad \text{with } a_i,b_i\in\mathbb{Z}_2.$$

This implies

$$f_1=\bigoplus_{i=1}^{s_1-1}(u_i\oplus b_iv_{s_1})(v_i\oplus a_iv_{s_1}) \pmod{B_{n,1}}.$$

Moreover,

$$\bigoplus_{i=s_2+1}^{s_1} u_iv_i=\bigoplus_{i=s_2+1}^{s_1-1}(u_i\oplus b_iv_{s_1})(v_i\oplus a_iv_{s_1}) \oplus v_{s_1}\left(u_{s_1}\oplus\bigoplus_{i=s_2+1}^{s_1-1}(a_iu_i\oplus b_iv_i)\right) \pmod{B_{n,1}}.$$

This yields a new representation for f_1,f_2 by formulae (4.1), (4.2) with

$$s_1^{\text{new}}=s_1-1, \qquad s_2^{\text{new}}=s_2, \qquad u_{s_1}^{\text{new}}=u_{s_1}\oplus\bigoplus_{i=s_2+1}^{s_1-1}(a_iu_i\oplus b_iv_i),$$

$$u_i^{\text{new}}=u_i\oplus b_iv_{s_1}, \qquad v_i^{\text{new}}=v_i\oplus a_iv_{s_1} \quad \text{for } i=1,\dots,s_1-1.$$

We can repeat this transformation at most s times since each step decreases the number s_2-s_1. If this transformation is not applicable we have

$$L(f_1)=s_1 \text{ and } L(f_2)=s-s_2.$$

In this situation we can take for g the function $g=\bigoplus_{i=s_2+1}^{s_1}u_iv_i$ as has been explained above. □

A quadratic form h *helps* in computing f if $L(f)=L(f\oplus h)+L(h)$. Thus the quadratic form g in Theorem 4.1 helps in computing both f_1 and f_2. In order to find such a form g it is important to have for fixed f a neat description of all pairs of linear forms u,v such that uv helps in computing f. By Corollary 3.8 these forms u,v must satisfy $D(uv)\subset D(f)$, and thus $u,v\in D(f)$. Theorem 4.2 characterizes the set of these linear forms u,v in the case that f is a canonical form.

We associate with the canonical form $f=\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}$ the bilinear form

$$\Phi_f: B_{2t,1}^2 \to \mathbb{Z}_2, \qquad \Phi_f(u,v)=\bigoplus_{i=1}^{t}(u_{2i-1}v_{2i} \oplus u_{2i}v_{2i-1}),$$

where $u_i, v_i \in \mathbb{Z}_2$ are the coordinates of $u=\bigoplus_{i=1}^{2t} u_i x_i$ and $v=\bigoplus_{i=1}^{2t} v_i x_i$. $\Phi_f(u,v)$ is the parity of the number of monomials $x_{2i-1}x_{2i}$ with $1 \leqslant i \leqslant t$ of uv. By definition $x_i x_j$ is a *monomial* of the quadratic form $\bigoplus_{i,j} c_{ij}x_i x_j$ iff $c_{ij} \oplus c_{ji}=1$. Let A be a matrix representing the canonical form f, i.e. $f=f_A$ then

$$\Phi_f(u,v)=u(A \oplus A^{\mathrm{T}})v^{\mathrm{T}}$$

holds for all $u,v \in B_{2t,1}$.

Theorem 4.2. *For the canonical form $f=\bigoplus_{i=1}^{t} x_{2i}x_{2i-1}$ and $u,v \in D(f)$ we have $L(f \oplus uv)=t-1$ iff uv has an odd number of the monomials $x_{2i-1}x_{2i}$ with $1 \leqslant i \leqslant t$, i.e. iff $\Phi_f(u,v)=1$.*

Proof. We first consider the case that $x_1 x_2$ is a monomial of uv and we later on reduce the general to this special case. We are going to simplify u by various isomorphic transformations without changing $f \pmod{B_{2t,1}}$. We can achieve $u_1=1$ and $v_1=0$ by possibly interchanging u and v, and the variables x_1, x_2. Next we apply various isomorphisms T_j on $\mathbb{Z}_2^{2t}$ for $j=3,\ldots,2t$ that are defined by the substitution steps

$$T_j^*: \begin{cases} x_1 := x_1 \oplus x_j & \\ x_{j-1} := x_{j-1} \oplus x_2 & \text{if } j \text{ is even.} \\ x_{j+1} := x_{j+1} \oplus x_2 & \text{if } j \text{ is odd} \end{cases}$$

We see that the forms $u^{\mathrm{new}}=T_j^*(u)$ and $v^{\mathrm{new}}=T_j^*(v)$ have the new coefficients

$$u_2^{\mathrm{new}}=\begin{cases} u_2 \oplus u_{j-1} & \text{if } j \text{ is even} \\ u_2 \oplus u_{j+1} & \text{if } j \text{ is odd,} \end{cases} \qquad v_2^{\mathrm{new}}=\begin{cases} v_2 \oplus v_{j-1} & \text{if } j \text{ is even} \\ v_2 \oplus v_{j+1} & \text{if } j \text{ is odd,} \end{cases}$$

$$u_j^{\mathrm{new}}=u_j \oplus 1.$$

The other coefficients u_i, v_i remain unchanged. The transformation T_j does not change the canonical form f and preserves the condition $u_1=1$, $v_1=0$. It is important that T_j preserves $\Phi_f(u,v)$, the parity of the number of monomials $x_{2i-1}x_{2i}$ of uv. This can be seen immediately since $u_1=1$, $v_1=0$, $j \geqslant 3$.

We recursively apply T_j for the minimal number $j \geqslant 3$ with $u_j=1$. In this way we transform u into either x_1 or $x_1 \oplus x_2$. In the latter case the substitution $x_1 := x_1 \oplus x_2$ finally transforms u into x_1. Therefore, we can assume w.l.o.g. that $u=x_1$ and in this case we have

$$f \oplus uv = x_1(x_2 \oplus v) \oplus \bigoplus_{i=2}^{t} x_{2i-1}x_{2i}.$$

We see that the following statements are equivalent:

(a) $v_2=0$,

(b) $\bigoplus_{i=1}^{t}(u_{2i-1}v_{2i}\oplus u_{2i}v_{2i-1})=0$,

(c) the linear forms $x_1, x_2\oplus v, x_3, \ldots, x_{2t}$ are linearly independent,

(d) $L(f\oplus uv)=t$.

The equivalence (a)$\Leftrightarrow$(b)$\Leftrightarrow$(c) is obvious; the equivalence (c)$\Leftrightarrow$(d) follows from Theorem 3.4 and $L=L_1$. Conversely, these equivalences imply the claim

$$\Phi_f(u,v)=1 \text{ iff } L(f\oplus uv)=t-1.$$

Now we reduce the general case to the case that x_1x_2 is a monomial of uv. If uv is linear then either $u=0$ or $v=0$ or $u=v$; the claim is trivial in each of these cases. It remains to consider the case that uv is nonlinear. Suppose that x_ix_j with $i<j\leqslant n$ is a monomial of uv. By permuting the variable groups $\{x_{2i-1}, x_{2i}\}$ for $i=1,\ldots,t$ and interchanging variables x_{2i-1}, x_{2i} we can transform uv, without changing f (mod $B_{2t,1}$), such that either x_1x_2 or x_2x_3 is a monomial of uv. If x_2x_3 is a monomial but x_1x_2 is not a monomial of uv, we apply the following substitution

$$x_3:=x_3\oplus x_1, \qquad x_2:=x_2\oplus x_4.$$

This substitution does not change f (mod $B_{2t,1}$) and transforms uv such that x_1x_2 becomes a monomial of uv. The substitution adds to uv the monomials x_1x_2, x_3x_4 and further monomials that are not of the type $x_{2i-1}x_{2i}$. Therefore, $\Phi_f(u,v)$, the parity of the number of monomials $x_{2i-1}x_{2i}$ of uv, remains unchanged. □

Remark. In the proof of Theorem 4.2 we have transformed the pair (f, uv) into a pair (f, x_1w) with $w\in B_{2t,1}$. We can continue this transformation and transform w into either x_2 or x_3 without changing f and x_1. We conclude that every pair (f, g) of quadratic forms with $D(g)\subset D(f)$, $L(f)=t$ and $L(g)=1$ is isomorphic to either the pair $(\bigoplus_{i=1}^{t}x_{2i-1}x_{2i}, x_1x_2)$ or to the pair $(\bigoplus_{i=1}^{t}x_{2i-1}x_{2i}, x_1x_3)$. Here by definition two pairs (f_1,f_2), $(\bar{f}_1,\bar{f}_2)$ of n-ary quadratic forms are *isomorphic* if there is an isomorphism T on $\mathbb{Z}_2^n$ such that $\bar{f}_i=f_iT$ (mod $B_{n,1}$) for $i=1,2$.

Definition. Let f be a quadratic form and let $U\subset D(f)$ be a linear subspace. We call f *nonlinear on* U if there exist $u,v\in U$ with $L(f\oplus uv)=L(f)-1$; otherwise, we call f *linear on* U.

This notion of linearity is justified by the following theorem.

Theorem 4.3. *Let $f\in B_{n,2}$ with $L(f)=t$ and let $U\subset D(f)$ be a linear subspace with* $\dim U=r$. *f is linear on U if and only if we can write $f=\bigoplus_{i=1}^{t}u_iv_i$ (mod $B_{n,1}$) with linearly independent linear forms $u_1,\ldots,u_t, v_1,\ldots,v_t$ so that $u_1,\ldots,u_r$ is a basis of U.*

Proof. We can assume that $f=f_A$ is the canonical form with $L(f_A)=t$ and $n=2t$.

("⇒"): Let f be linear on U. We construct the desired representation of f by induction on $\dim U$. The claim is trivial if $\dim U=0$. We know from Theorem 4.2 that the equivalence

$$L(f\oplus uv)=t-1 \Leftrightarrow u(A\oplus A^{\mathrm{T}})v^{\mathrm{T}}=1$$

holds for all $u,v\in B_{2t,1}$. Since $\mathrm{R}(A\oplus A^{\mathrm{T}})=2t$, we can choose any nonzero $u_1\in B_{2t,1}$ and we can find $v_1\in B_{2t,1}$ such that $u_1(A\oplus A^{\mathrm{T}})v_1^{\mathrm{T}}=1$. If $u_1\in U$ and f is linear on U then v_1 cannot be in U. We apply the induction hypothesis to $\bar{f}=f\oplus u_1v_1 \pmod{B_{2t,1}}$ and $\bar{U}:=U\cap D(\bar{f})$. We see from $\dim D(\bar{f})=\dim D(f)-2$ and $u_1,v_1\notin D(\bar{f})$, $u_1\in U$, $v_1\notin U$ that $\dim\bar{U}=\dim U-1$. The construction obviously implies that $\bar{f}$ is linear on $\bar{U}$. By induction hypothesis there is a desired representation for $\bar{f}$ and $\bar{U}$:

$$\bar{f}=\bigoplus_{i=2}^{t} u_iv_i \pmod{B_{2t,1}}.$$

From this we obtain the desired representation for f:

$$f=\bigoplus_{i=1}^{t} u_iv_i \pmod{B_{2t,1}}.$$

In fact, $u_1,\ldots,u_r$ is a basis for U since $u_2,\ldots,u_r$ is a basis for $\bar{U}$, $u_1\in U-\bar{U}$ and $\dim U=\dim\bar{U}+1$.

("⇐"): Let $f=\bigoplus_{i=1}^{t}u_iv_i \pmod{B_{n,1}}$ with linearly independent linear forms $u_1,\ldots,u_t,v_1,\ldots,v_t$ and $U=\langle u_1,\ldots,u_r\rangle$. Without loss of generality, we can assume that $u_i=x_{2i-1}$, $v_i=x_{2i}$ for $i=1,\ldots,t$. This is because we can transform $u_1,\ldots,v_t$ by a linear isomorphism into $x_1,\ldots,x_{2t}$. Now it follows from Theorem 4.2 that f is linear on $U=\langle x_{2i-1}\mid i=1,\ldots,r\rangle$. For if $u,v\in U$ we cannot have $L(f\oplus uv)=L(f)-1$ since uv has no monomial of the form $x_{2i-1}x_{2i}$. □

We call two quadratic forms f_1,f_2 (*weakly*) *computationally independent* if $L_1(f_1,f_2)=L(f_1)+L(f_2)$. Theorem 4.4 shows that f_1,f_2 are computationally independent iff either f_1 or f_2 is linear on $D(f_1)\cap D(f_2)$.

Theorem 4.4. *Let f_1,f_2 be quadratic forms in $B_{n,2}$, $U=D(f_1)\cap D(f_2)$. Then the following holds.*

(1) *$L_1(f_1,f_2)=L(f_1)+L(f_2)$ iff either f_1 or f_2 is linear on U.*

(2) *If $L_1(f_1,f_2)<L(f_1)+L(f_2)$, we can find, in polynomial time, linear forms $u,v\in B_{n,1}$ such that $L(f_i\oplus uv)=L(f_i)-1$ for $i=1,2$.*

Proof. Suppose that $L_1(f_1,f_2)<L(f_1)+L(f_2)$. By Theorem 4.1 there exists a quadratic form g such that $L_1(f_1,f_2)=L(f_1\oplus g)+L(f_2\oplus g)+L(g)$ and $L(f_i)=L(f_i\oplus g)+L(g)$. We know from Corollary 3.8 that $D(f_i)=D(g)\times D(f_i\oplus g)$ for $i=1,2$. We see from $L(g)\geqslant 1$ that f_1 and f_2 are nonlinear on U. This proves the "if"-part of the equivalence (1).

Next we show how to find in polynomial time, linear forms $u, v \in B_{n,1}$ such that $L(f_i \oplus uv) = L(f_i) - 1$ for $i = 1, 2$. We know from Corollary 3.8 that these forms satisfy $u, v \in U = D(f_1) \cap D(f_2)$.

By Theorem 4.2 and since f_1, f_2 are isomorphic to canonical forms there exist bilinear forms $\Phi_{f_i}(u, v)$ $i = 1, 2$ such that for all $u, v \in D(f_i)$

$$\Phi_{f_i}(u, v) = 1 \text{ iff } L(f_i \oplus uv) = L(f_i) - 1.$$

To find Φ_{f_i} we construct an isomorphism T_i on $\mathbb{Z}_2^n$ that transforms f_i into the corresponding canonical form $\bar{f}_i$, i.e. $\bar{f}_i = f_i T_i \pmod{B_{n,1}}$. Then the bilinear form Φ_{f_i} is determined by

$$\Phi_{f_i}(u, v) = \Phi_{\bar{f}_i}(uT_i, vT_i) \quad \text{for all } u, v \in D(f_i),$$

where the bilinear form $\Phi_{\bar{f}_i}$ associated with the canonical form $\bar{f}_i$ is given by Theorem 4.2. To obtain the matrix representation for $\Phi_{\bar{f}_i}$ we use a matrix A_i representing the canonical form $\bar{f}_i = f_{A_i}$ and the matrix τ_i representing the transformation T_i. We know from Theorem 4.2 that the bilinear form $\Phi_{\bar{f}_i}$ is represented by the matrix $A_i \oplus A_i^{\mathsf{T}}$, i.e. for all $u, v \in B_{n,1} = M_{1,n}(\mathbb{Z}^2)$

$$\Phi_{\bar{f}_i}(u, v) = u(A_i \oplus A_i^{\mathsf{T}})v^{\mathsf{T}}.$$

It follows that the bilinear form $\Phi_{\bar{f}_i}(uT, vT)$ is represented by the matrix

$$M_i := \tau_i(A_i \oplus A_i^{\mathsf{T}})\tau_i^{\mathsf{T}}.$$

Without loss of generality, let $U = \langle x_1, \ldots, x_r \rangle$ for some integer r; then we have $u_j = v_j = 0$ for $j = r+1, \ldots, n$ for all $u, v \in U$. In order to find $u, v \in U$ such that $L(f_i \oplus uv) = L(f_i) - 1$ for $i = 1, 2$ we have to solve the equations

$$uM_i v^{\mathsf{T}} = 1 \quad u, v \in U \quad \text{for } i = 1, 2.$$

Let $\bar{M}_i$ be the submatrix of M_i consisting of rows and columns $1, \ldots, r$. The matrix $\bar{M}_i$ is nonzero since f_i is nonlinear on U. Therefore, the sets

$$U_i = \{u \in U \mid u\bar{M}_i = (0, \ldots, 0)\}$$

for $i = 1, 2$ are proper subspaces of U. We have $\# U_1, \# U_2 \leqslant \# U/2$ and, since $U_1 \cap U_2 \neq \emptyset$, this shows that $U_1 \cup U_2$ is properly contained in U. To find a form $u \in U - U_1 \cup U_2$, we construct a basis $w_1, \ldots, w_r$ of U such that $w_1, \ldots, w_s$ is a basis of $U_1 \cap U_2$ and $w_1, \ldots, w_t$ is a basis of U_1. It can easily be seen that $u := w_t \oplus w_r$ is not in $U_1 \cup U_2$. We can find u in polynomial time. For this u the sets

$$V_{i,u} = \{v \in U \mid u\bar{M}_i v^{\mathsf{T}} = 0\}$$

for $i = 1, 2$ are proper subspaces of U, and thus $V_{1,u} \cup V_{2,u}$ does not cover U. We can find $v \in U - V_{1,u} \cup V_{2,u}$ by solving the two linear equations $u\bar{M}_i v^{\mathsf{T}} = 1$ for $i = 1, 2$. This proves (2) since we can find u, v in polynomial time.

It remains to prove the "only if"-part of the equivalence (1). This follows from the above proof. We have shown the existence of $u, v \in U$ such that $L(f_i \oplus uv) = L(f_i) - 1$ for $i = 1, 2$ provided that f_1 and f_2 are nonlinear on U. □

We give two examples. The functions

$$f_1 = x_1 x_2 \oplus x_3 x_4, \qquad f_2 = x_1 x_3 \oplus x_2 x_4$$

are both nonlinear on $B_{4,1} = D(f_1) \cap D(f_2)$. By Theorem 4.4(1) this implies $L_1(f_1, f_2) \leqslant 3$. A corresponding circuit with 3 $\wedge$-gates is as follows.

$$f_1 = x_1(x_2 \oplus x_3) \oplus x_3(x_4 \oplus x_1), \qquad f_2 = x_1(x_2 \oplus x_3) \oplus x_2(x_4 \oplus x_1).$$

This example is quite similar to the well-known multiplication of two complex numbers using three real multiplications.

On the other hand, by Theorem 4.4(1) the functions

$$f_1 = x_1 x_2 \oplus x_3 x_4 \oplus \cdots \oplus x_{4t-1} x_{4t}, \qquad f_2 = x_2 x_3 \oplus x_6 x_7 \oplus \cdots \oplus x_{4t-2} x_{4t-1}$$

are computationally independent since f_1 depends linearly on the variables of f_2. This shows that

$$L_1(f_1, f_2) = 3t.$$

The L_1-complexity of (f_1, f_2) is maximal for all pairs of forms $f_1, f_2 \in B_{4t,2}$, as follows from Theorem 4.5.

Theorem 4.5. $\max\{L_1(f_1, f_2) \mid f_1, f_2 \in B_{n,2}\} = \lfloor 3n/4 \rfloor$.

Proof. Let $(f_1, f_2) \in B_{n,2}^2$ be any pair with maximal L_1-complexity. According to Theorem 4.1 there exists a form $g \in B_{n,2}$ such that

$$L_1(f_1, f_2) = L(f_1 \oplus g) + L(f_2 \oplus g) + L(g),$$

$$L(f_i) = L(f_i \oplus g) + L(g) \quad \text{for } i = 1, 2.$$

Since $f_1 \oplus g, f_2 \oplus g$ are computationally independent, we know from Theorem 4.4(1) that either $f_1 \oplus g$ or $f_2 \oplus g$ is linear on $U := D(f_1 \oplus g) \cap D(f_2 \oplus g)$. By symmetry we can assume that $f_2 \oplus g$ is linear on U.

Then there exist in $B_{n,1}$ linearly independent linear forms x_i, y_i for $i = 1, \ldots, r$, u_j, v_j for $j = 1, \ldots, s$ and w_k for $k = 1, \ldots, t$ such that

$$g = \bigoplus_{i=1}^{r} x_i y_i, \qquad f_1 \oplus g = \bigoplus_{j=1}^{s} u_j v_j, \qquad f_2 \oplus g = \bigoplus_{k=1}^{t} u_k w_k.$$

The particular form of $f_1 \oplus g$, $f_2 \oplus g$ is a consequence of Theorem 4.3. We have

$$n \geqslant 2r+2s+t, \quad t \leqslant s \leqslant n/2$$

$$L(f_1,f_2)=r+s+t \leqslant \frac{n}{2}+\frac{t}{2} \leqslant \frac{3}{4}n.$$

Hence $L(f_1,f_2) \leqslant \lfloor \frac{3}{4}n \rfloor$. □

The final theorem of this section shows that the complexity measures L and L_1 coincide for pairs of quadratic forms. Thus all the previous characterizations of $L_1(f_1,f_2)$ also hold for $L(f_1,f_2)$.

Theorem 4.6. *$L(f_1,f_2)=L_1(f_1,f_2)$ for all $f_1,f_2 \in B_{n,2}$.*

Proof. By Theorem 4.1 there exists a quadratic form $g \in B_{n,2}$ such that

$$L(f_i)=L(f_i \oplus g)+L(g) \quad \text{for } i=1,2 \quad \text{and}$$

$$L_1(f_1,f_2)=L(f_1 \oplus g)+L(f_2 \oplus g)+L(g).$$

Let $U=D(f_1 \oplus g) \cap D(f_2 \oplus g)$. By Theorem 4.4 either $f_1 \oplus g$ or $f_2 \oplus g$ is linear on U. By symmetry we can suppose that $f_2 \oplus g$ is linear on U. Let $r=\dim U$, and $t_2=L(f_2 \oplus g)$; we can assume w.l.o.g. that $B_{n,1}$ is the span of $D(f_1) \cup D(f_2)$. By Theorem 4.3 there exist linearly independent forms $u_1,\ldots,u_r \in U$ and $v_1,\ldots,v_{2t_2-r} \in B_{n,1}$ such that

$$f_2 = \bigoplus_{i=1}^{r} u_i v_i \oplus \bigoplus_{i=1}^{t_2-r} v_{2i-1+r} v_{2i+r} \oplus g \pmod{B_{n,1}}. \tag{4.3}$$

Without loss of generality, we assume that $u_1,\ldots,u_r$ and $v_1,\ldots,v_{2t_2-r}$ are boolean variables. This can be achieved by applying to f_1,f_2 a suitable isomorphism.

We are going to eliminate from an arbitrary circuit for f_1,f_2 at least $t_2=L(f_2 \oplus g)$ $\wedge$-gates in such a way that the transformed circuit still computes f_1. This clearly proves

$$L(f_1,f_2) \geqslant L(f_1)+L(f_2 \oplus g)=L_1(f_1,f_2).$$

To this end we successively substitute boolean functions for the variables $v_1,\ldots,v_{2t_2-r}$. Consider a first $\wedge$-gate of the given circuit for f_1,f_2 that depends on some of the variables $v_1,\ldots,v_{2t_2-r}$, and let it depend on v_i. At least one of the inputs of this $\wedge$-gate depends on v_i and it depends linearly on v_i. Thus this input is of the form $v_i \oplus w \oplus h$, where $w \in \langle v_1,\ldots,v_{2t_2-r} \rangle$ is a linear form that does not depend on v_i, and $h \in B_n$ does not depend on the variables $v_1,\ldots,v_{2t_2-r}$.

We transform f_1, f_2 and the given circuit according to the substitution $v_i := w \oplus h$. The transformed circuit first computes $w \oplus h$ and then replaces in all steps v_i by $w \oplus h$. The above $\wedge$-gate with input $v_i \oplus w \oplus h$ will be eliminated.

The substitution $v_i := w \oplus h$ does not change f_1 and g. This is because neither $f_1 \oplus g$ nor g depend on v_i. The substitution may transform f_2 into a polynomial of arbitrary degree.

The substitution $v_i := w \oplus h$ transforms the term yv_i in (4.3) into $yw \oplus yh$, where

$$y = \begin{cases} u_i & \text{if } i \leqslant r, \\ v_{i-1} & \text{if } i > r,\ i-r \text{ is even}, \\ v_{i+1} & \text{if } i > r,\ i-r \text{ is odd}. \end{cases}$$

The substitution $v_i := w \oplus h$ eliminates one of the t_2 products, namely yv_i, from

$$(4.4) \qquad f_2 \oplus g = \bigoplus_{i=1}^{r} u_i v_i \oplus \bigoplus_{i=1}^{t_2 - r} v_{2i-1+r} v_{2i+r}$$

and replaces it by $yh \oplus yw$. We can continue to eliminate $\wedge$-gates from the circuit until the remaining $t_2 - 1$ terms of the quadratic form (4.4) have all been cancelled. Each elimination step cancels at most one of the products in (4.4). It is important that the further elimination steps will not affect the new term $yh \oplus yw$. This is because h does not depend on any of the variables v_j that are substituted later on, and since y remains unchanged. We also use that the additional terms $yh \oplus yw$ do not interfere with the remaining $t_2 - 1$ products in (4.4), for $f_2 \oplus g \oplus yv_i$ does not depend on the variable y. Therefore, we can at least eliminate $t_2 = L(f_2 \oplus g)$ $\wedge$-gates from the given circuit and the transformed circuit still computes f_1. □

5. On the complexity of sets of quadratic forms

Theorem 5.1. *For every r with $9 \leqslant r \leqslant n/9$ the fraction of r-tuples $(f_1, \ldots, f_r) \in B^r_{n,2}$ which satisfy $L(f_1, \ldots, f_r) \leqslant n\sqrt{r}/3$ is at most $2^{-nr/2}$.*

Proof. Every computation for $f_1, \ldots, f_r$ with at most t multiplications can be expressed by boolean functions h_i, k_i, g_i for $i = 1, \ldots, t$ such that

$$(5.1) \qquad \begin{aligned} &h_1, k_1 \in \langle x_1, \ldots, x_n \rangle, && g_1 = h_1 k_1 \quad \text{and} \\ &h_i, k_i \in \langle g_1, \ldots, g_{i-1}, x_1, \ldots, x_n \rangle, && g_i = h_i k_i \quad \text{for } i = 2, \ldots, t. \end{aligned}$$

$$(5.2) \qquad f_1, \ldots, f_r \in \langle g_1, \ldots, g_t, x_1, \ldots, x_n \rangle.$$

We have 2^{n+i-1} choices for each of h_i and k_i; this gives at most $2^{2n+2i-3}$ distinct functions $g_i = h_i k_i \pmod{B_{n,1}}$. We see that there are at most 2^{2nt+t^2} t-tuples $(g_1, \ldots, g_t)$

and thus we have at most 2^{2nt+t^2+rt} r-tuples $(f_1,\dots,f_r)\in B_{n,2}^r$ such that $L(f_1,\dots,f_r)\leqslant t$. On the other hand,

$$|B_{n,2}|^r=2^{(n^2-n)r/2}.$$

To prove the claim it remains to verify the inequality

$$2nt+t^2+rt<(n^2-n)r/2-nr/2$$

for $t\leqslant n\sqrt{r}/3$ and $9\leqslant r\leqslant n/9$. This inequality holds for all $t\leqslant n\sqrt{r}/3$ since it holds for $t=n\sqrt{r}/3$ provided that $n\geqslant 81$. □

We know from Sections 3 and 4 that the complexity measures L and L_1 coincide for single quadratic forms and for pairs of quadratic forms. It is open whether $L(f_1,\dots,f_r)=L_1(f_1,\dots,f_r)$ holds for all sets of quadratic forms $f_1,\dots,f_r$. It is not known whether the use of nonquadratic polynomials can decrease the number of $\wedge$-gates in circuits for sets of quadratic forms. Computations which do not use higher-degree polynomials are computations with all multiplications on the first level.

By Theorem 5.1 the circuit complexity of almost all sets of n-ary quadratic boolean forms $f_1,\dots,f_r$ is nonlinear in n. Sets of quadratic forms are the simplest type of n-ary boolean functions with this property. For instance, an easy argument shows that every set of r n-ary linear boolean forms can be computed with no more than 2^r+n-2 additions. Therefore, the circuit complexity of $(\log n)$-tuples of n-ary linear forms is at most $2n$. On the other hand, the L-complexity of higher-degree boolean polynomials is harder to analyze than that of quadratic forms. We conclude that sets of quadratic boolean forms are the right test point for either proving nonlinear circuit complexity lower bounds or for understanding the reasons that such bounds may be unprovable.

Strassen [11] observed that the multiplicative complexity of a set of quadratic forms is closely related to the rank of a corresponding tensor. We adapt Strassen's exposition to boolean forms. We define the *rank* $\mathrm{R}(\mathfrak{A})$ of an r-tuple $\mathfrak{A}=(A_1,\dots,A_r)$ of boolean $n\times n$ matrices as the minimal integer t for which there exist $n\times n$ matrices $T_1,\dots,T_t$ with rank 1 such that $A_1,\dots,A_r\in\langle T_1,\dots,T_t\rangle$. There is a natural way to identify $\mathfrak{A}$ with an $n\times n\times r$ tensor.

Theorem 5.2(1) shows that the L_1-complexity of the quadratic forms $f_{A_1},\dots,f_{A_r}$ equals the minimal rank of all tensors $\mathfrak{A}\oplus\mathfrak{S}$, where $\mathfrak{S}$ ranges over all symmetric tensors. Therefore, lower bounds to the L-complexity of sets of quadratic forms also hold for the ranks of all corresponding tensors $\mathfrak{A}\oplus\mathfrak{S}$. So far we do not have any example of a sequence of $n\times n\times r$ tensors with coefficients in $\mathbb{Z}_2$ such that a lower rank bound has been proven that is nonlinear in $n+r$. Proving nonlinear lower bounds to the tensor rank by itself may be an infeasible task. By Theorem 5.2 this task is easier than proving nonlinear lower bounds on the L-complexity of sets of quadratic forms. On the other hand, if nonlinear lower bounds to the tensor rank are provable, then nonlinear lower bounds to the L_1-complexity are most likely provable, too. This

follows from the lower bound in Theorem 5.2(2) and the observation that $R(\mathfrak{A} \oplus \mathfrak{A}^T) \geq nr/9$ for almost all $n \times n \times r$ tensors $\mathfrak{A}$.

Theorem 5.2 (cf. Strassen [11, Section 4, Theorem 4 and Corollary 5]). *For every r-tuple $\mathfrak{A} = (A_1, \ldots, A_r)$ of boolean $n \times n$ matrices the following holds.*

(1) $L_1(f_{A_1}, \ldots, f_{A_r}) = \min\{R(\mathfrak{A} \oplus \mathfrak{S}) \mid \mathfrak{S} = \mathfrak{S}^T\}$, *where the minimum is taken over all r-tuples $\mathfrak{S} = (S_1, \ldots, S_r)$ of symmetric $n \times n$ matrices. Here let $\mathfrak{A} \oplus \mathfrak{S} = (A_1 \oplus S_1, \ldots, A_r \oplus S_r)$.*

(2) $\frac{1}{2}R(\mathfrak{A} \oplus \mathfrak{A}^T) \leq L_1(f_{A_1}, \ldots, f_{A_r})$.

Proof. (1) ("$\leq$"): Suppose there exist rank-1 matrices $T_1, \ldots, T_t$ and symmetric matrices $S_1, \ldots, S_r$ such that

$$A_1 \oplus S_1, \ldots, A_r \oplus S_r \in \langle T_1, \ldots, T_t \rangle.$$

Applying the homomorphism $\psi : M_{n,n}(\mathbb{Z}_2) \to B_{n,2}$ with $\psi(A) = f_A$ yields

$$f_{A_1}, \ldots, f_{A_r} \in \langle f_{T_1}, \ldots, f_{T_t} \rangle.$$

Since $L(f_{T_i}) \leq 1$ for $i = 1, \ldots, t$, this implies $L_1(f_{A_1}, \ldots, f_{A_r}) \leq t$.

("$\geq$"): If $L_1(f_{A_1}, \ldots, f_{A_r}) \leq t$ then there exist linear forms $u_i, v_i \in B_{n,1}$ for $i = 1, \ldots, t$ such that

$$f_{A_1}, \ldots, f_{A_r} \in \langle u_1 v_1, \ldots, u_t v_t, x_1, \ldots, x_n \rangle.$$

There exist matrices T_i such that $u_i v_i = f_{T_i} \pmod{B_{n,1}}$ and $R(T_i) = 1$ for $i = 1, \ldots, t$. This implies

$$f_{A_1}, \ldots, f_{A_r} \in \langle f_{T_1}, \ldots, f_{T_t} \rangle.$$

Since the kernel of ψ consists of symmetric matrices there exist symmetric matrices $S_1, \ldots, S_t$ such that

$$A_1 \oplus S_1, \ldots, A_r \oplus S_r \in \langle T_1, \ldots, T_t \rangle.$$

Hence $R(\mathfrak{A} \oplus \mathfrak{S}) \leq t$.

(2) We know from (1) that there exist symmetric matrices $S_1, \ldots, S_r$ such that $R(\mathfrak{A} \oplus \mathfrak{S}) = L_1(f_{A_1}, \ldots, f_{A_r})$ holds for $\mathfrak{S} = (S_1, \ldots, S_r)$. It can easily be seen that

$$R(\mathfrak{A} \oplus \mathfrak{S}) = R(\mathfrak{A}^T \oplus \mathfrak{S}^T).$$

By the subadditivity of the rank we have

$$\begin{aligned} R(\mathfrak{A} \oplus \mathfrak{A}^T) &= R(\mathfrak{A} \oplus \mathfrak{S} \oplus \mathfrak{A}^T \oplus \mathfrak{S}^T) \\ &\leq R(\mathfrak{A} \oplus \mathfrak{S}) + R(\mathfrak{A}^T \oplus \mathfrak{S}^T) \\ &\leq 2R(\mathfrak{A} \oplus \mathfrak{S}) = 2L_1(f_{A_1}, \ldots, f_{A_r}). \end{aligned}$$

□

By Theorem 3.4 we have

$$L_1(f_A)=\tfrac{1}{2}\mathrm{R}(A\oplus A^{\mathrm{T}}).$$

It is open whether this equality extends to the equality

$$L_1(f_{A_1},\ldots,f_{A_r})=\tfrac{1}{2}\mathrm{R}(\mathfrak{A}\oplus\mathfrak{A}^{\mathrm{T}}),$$

with $\mathfrak{A}=(A_1,\ldots,A_r)$ for arbitrary sets of quadratic forms $f_{A_1},\ldots,f_{A_r}$.

The following result shows that $L_1(f_1,\ldots,f_r)$ is at least twice the average complexity of the functions in the subspace $\langle f_1,\ldots,f_r\rangle$ generated by $f_1,\ldots,f_r$.

Theorem 5.3. *Let $\langle f_1,\ldots,f_r\rangle\subset B_{n,2}$ be the subspace that is generated by the quadratic forms $f_1,\ldots,f_r$. Then $L_1(f_1,\ldots,f_r)\geqslant 2^{1-r}\sum_{f\in\langle f_1,\ldots,f_r\rangle}L(f)$.*

Proof. Let $L_1(f_1,\ldots,f_r)=t$. Then there exist forms $h_1,\ldots,h_t\in B_{n,2}$ with $L(h_i)=1$ for $i=1,\ldots,t$ such that

$$\langle f_1,\ldots,f_r\rangle\subset\langle h_1,\ldots,h_t\rangle.$$

Thus, for all $f\in\langle f_1,\ldots,f_r\rangle$ we can write

$$f=\bigoplus_{i=1}^{t}a_{f,i}h_i,\quad\text{with } a_{f,i}\in\mathbb{Z}_2,$$

where for every i the map $f\mapsto a_{f,i}$ is a nontrivial homomorphism. Hence, for every i the coefficient $a_{f,i}$ is 0 (resp. 1) for exactly half of the f in $\langle f_1,\ldots,f_r\rangle$, i.e.

$$\#\{f\in\langle f_1,\ldots,f_r\rangle\mid a_{f,i}=1\}\leqslant 2^{r-1}.$$

Summing this equality for $i=1,\ldots,t$ gives

$$\sum_{f\in\langle f_1,\ldots,f_r\rangle}L(f)\leqslant t2^{r-1}$$

since $L(f)\leqslant\#\{i\mid a_{f,i}=1\}$. This proves the claim. □

Corollary 5.4. *Let $f_s=\bigoplus_{i=0}^{t-1}x_{2i+1}x_{2i+2s}\in B_{2t+2r}$ for $s=1,\ldots,r$. Then*

$$L_1(f_1,\ldots,f_r)\geqslant 2t(1-2^{-r}).$$

Proof. We first show that $L(f)=t$ holds for all nonzero forms f in $\langle f_1,\ldots,f_r\rangle$. The form $f=\bigoplus_{s=1}^{r}a_sf_s$ can be written as

$$f=\bigoplus_{i=0}^{t-1}x_{2i+1}\left(\bigoplus_{s=1}^{r}a_sx_{2i+2s}\right).$$

If $(a_1,\ldots,a_s)$ is nonzero then the linear forms x_{2i+1} and $\bigoplus_{s=1}^{r}a_sx_{2i+2s}$ for $i=1,\ldots,t$ are linearly independent. Hence $L(f)=t$ by Theorem 3.6.

Application of Theorem 5.3 yields

$$L_1(f_1,\dots,f_r)\geqslant 2t\cdot(2^r-1)2^{-r}=2t(1-2^{-r}). \qquad \square$$

The lower bound of Corollary 5.4 is sharp for $r=2$ and even t. We have

$$f_1=\bigoplus_{i=1}^{t} x_{2i-1}x_{2i}=\bigoplus_{i=1}^{t/2}(x_{4i-3}(x_{4i-2}\oplus x_{4i})\oplus x_{4i}(x_{4i-1}\oplus x_{4i-3}))$$

$$f_2=\bigoplus_{i=1}^{t} x_{2i-1}x_{2i+2}=\bigoplus_{i=1}^{t/2} x_{4i-3}(x_{4i-2}\oplus x_{4i})\oplus\bigoplus_{i=1}^{t/2} x_{4i-1}(x_{4i}\oplus x_{4i+2})\oplus f_1.$$

This gives an example of forms $f_1,f_2\in B_{n,2}$ with $n=0 \pmod 4$ such that $L_1(f_1,f_2)=\frac{3}{4}n$. We know from Theorem 4.5 that $\frac{3}{4}n$ is the maximal L_1-complexity for all pairs $f_1,f_2\in B_{n,2}$.

References

[1] N. Blum, A boolean function requiring $3n$ network size, *Theoret. Comput. Sci.* **14** (1984) 337–345.

[2] J. Ja'Ja', Optimal evaluation of pairs of bilinear forms, *SIAM J. Comput.* **8** (1979) 443–462.

[3] J. Ja'Ja', On the complexity of bilinear forms, *SIAM J. Comput.* **9** (1980) 713–728.

[4] R. Mirwald and C.P. Schnorr, The multiplicative complexity of quadratic boolean forms, in: *Proc. 28th IEEE Symp. on Foundations of Computer Science*, Los Angeles (1987), 141–149.

[5] R. Mirwald and C.P. Schnorr, Characterization of the rank of a pair of matrices over $\mathbb{Z}_2$, Preprint, Universität Frankfurt, 1990.

[6] M.S. Paterson, On Razborov's result for bounded-depth circuits over $\{\oplus, \wedge\}$, Preprint, University of Warwick, 1986.

[7] A.A. Razborov, Lower bounds on the size of bounded-depth networks over the basis $\{\wedge,\oplus\}$, To appear in *Matem. Zamatki*, Russian summary in *Uspekhi Mat. Nauk*, *T* **41**(4) (1986) 219–220.

[8] C.P. Schnorr, A $3n$-lower bound on the network complexity of Boolean functions, *Theoret. Comput. Sci.* **10** (1980) 83–92.

[9] C.P. Schnorr, A Gödel theorem on network complexity lower bounds, *Z. Math. Logik Grundlag. Math.* **32** (1986) 377–384.

[10] C.P. Schnorr, The multiplicative complexity of Boolean functions, in: *Proc. 1st Internat. Joint Conf. of ISSAC '88 and AAECC-6*, Rome (1988), Lecture Notes in Computer Science, Vol. 357 (Springer, Berlin, 1989) 45–58.

[11] V. Strassen, Vermeidung von Divisionen, *J. Reine Angew. Math.* **264** (1973) 184–202.

[12] V. Strassen, Algebraische Berechnungskomplexität, in: *Perspectives in Mathematics* (Birkhäuser Verlag, Basel, 1984).

[13] I. Wegener, *The complexity of boolean functions*, Wiley–Teubner Series in Computer Science (Teubner, Stuttgart, 1987 and Wiley, Chichester, UK, 1987).